#5

Atty. Dkt. No. 074273/0179

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Yukiyasu TSUNOO

Title: ENCRYPTION EVALUATION SUPPORT SYSTEM THAT CAN LARGELY REDUCE EVALUATION TIME OF ENCRYPTION ALGORITHM, AND RECORD MEDIUM RECORDING ITS PROGRAM

Appl. No.: Unassigned

Filing Date: 1/23/2001

Examiner: Unassigned

Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

- Japanese Patent Application No. 2000-017878 filed January 24, 2000.

Respectfully submitted,

Date January 23, 20001

By LYLE KIMMS
REG. NO. 34079
for David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

74273/179
TSUNOO
工藤
US

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

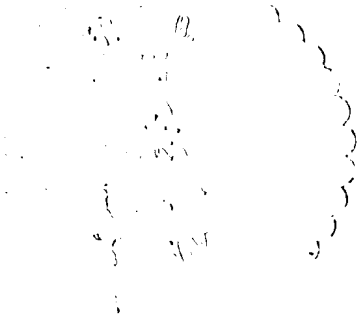
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月２４日

出願番号
Application Number: 特願２０００－０１７８７８

出願人
Applicant (s): 日本電気株式会社



２０００年１０月１３日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０８４３９９

【書類名】　特許願
【整理番号】　33509673
【提出日】　平成12年 1月24日
【あて先】　特許庁長官殿
【国際特許分類】　G09C 1/00
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　角尾　幸保
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100088959
　【弁理士】
　【氏名又は名称】　境　廣巳
【手数料の表示】
　【予納台帳番号】　009715
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9002136
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号評価支援システム及びプログラムを記録した機械読み取り可能な記録媒体

【特許請求の範囲】

【請求項１】　予め定義した暗号アルゴリズム仕様記述法で記述された暗号アルゴリズムの図形表現を格納する評価対象記憶部と、

前記暗号アルゴリズム仕様記述法で使う単位図形の点数を記憶する点数記憶部と、

前記評価対象記憶部から図形表現を入力し、該図形表現中の単位図形に対して前記点数記憶部に記憶された点数を付与し、予め定められた計算ルールに従って前記図形表現全体の得点を計算して出力する評価実施手段とを備えた暗号評価支援システム。

【請求項２】　前記評価実施手段が入力した図形表現中の利用者によって選択された単位図形を他の種類の単位図形に自動的に置き換えた図形表現を生成する自動組み替え手段を備え、前記評価実施手段は、前記入力した図形表現および前記自動組み替え手段で生成された図形表現について得点計算を行う請求項１記載の暗号評価支援システム。

【請求項３】　前記点数記憶部は予め定められた複数の評価項目の各々についてその評価項目の得点計算に使用する各単位図形の点数を記憶しており、前記評価実施手段は、利用者から指定された評価項目毎に、前記点数記憶部に記憶された評価項目別の各単位図形の点数を参照して得点計算を行う請求項１または２記載の暗号評価支援システム。

【請求項４】　前記複数の評価項目は、暗号強度に関する複数の評価項目を含む請求項３記載の暗号評価支援システム。

【請求項５】　前記評価実施手段は、各評価項目毎に、前記図形表現中の信号の流れに沿って基本ブロックを通過する毎にその基本ブロックの点数を加点することで得点計算を行う請求項４記載の暗号評価支援システム。

【請求項６】　前記点数記憶部に記憶される点数を単位図形のビット単位の点数とし、前記評価実施手段は、各評価項目毎に、前記図形表現の各出力ビット

毎の得点であるビット得点と、該ビット得点の平均値である項目得点とを算出する請求項５記載の暗号評価支援システム。

【請求項７】　前記暗号アルゴリズム仕様記述法による暗号アルゴリズムの図形表現を利用者が記述および編集するのを支援する評価対象編集手段を備えた請求項１、２、３、４、５または６記載の暗号評価支援システム。

【請求項８】　前記評価実施手段の計算結果を格納する評価結果記憶部と、該評価結果記憶部に格納された計算結果をグラフ化して出力する結果編集手段とを備えた請求項１、２、３、４、５または６記載の暗号評価支援システム。

【請求項９】　前記評価実施手段の計算結果を格納する評価結果記憶部と、該評価結果記憶部に格納された計算結果を指定されたソートキーでソートして出力する結果編集手段とを備えた請求項１、２、３、４、５または６記載の暗号評価支援システム。

【請求項１０】　コンピュータを、

予め定義した暗号アルゴリズム仕様記述法による暗号アルゴリズムの図形表現を利用者が記述および編集するのを支援する評価対象編集手段、

該評価対象編集手段で編集された暗号アルゴリズムの図形表現を格納する評価対象記憶部、

前記暗号アルゴリズム仕様記述法で使う単位図形の点数を予め定められた複数の評価項目毎に記憶する点数記憶部、

前記評価対象記憶部に格納された図形表現を入力し、利用者から指定された評価項目毎に、図形表現中の単位図形に対して前記点数記憶部に記憶された当該評価項目にかかる点数を付与して予め定められた計算ルールに従って図形表現全体の得点を計算して出力する評価実施手段、

として機能させるプログラムを記録した機械読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は暗号アルゴリズムの評価作業を支援する暗号評価支援システムに関する。

【０００２】

【従来の技術】

ネットワークの急速な普及に伴い、情報の漏洩を防止する暗号技術の重要性が年々高まっている。暗号には大別して、暗号化と復号化で同じ鍵を使う共通鍵暗号と、秘密鍵と公開鍵という異なる鍵を使用する公開鍵暗号とがある。共通鍵暗号は送受信者間で鍵を共有する方法が問題となるが、公開鍵暗号に比べて暗号化及び復号化に要する計算量が少ない利点があるため、多くの分野や用途で使用されている。

【０００３】

他方、暗号アルゴリズムに対する解読技術も急速に進歩しており、利用している暗号の安全性が永久に保証されるとは限られないのも事実である。従って、新しい解読技術に耐えられる新しい暗号アルゴリズムを積極的に設計し、事前にその強度を評価することが重要である。このための技術が従来より幾つか提案ないし実用化されている。

【０００４】

例えば、特開平１０－２４０５１１号公報（以下、文献１と称す）には、暗号アルゴリズムの設計を支援する従来技術の一例として、ビット列データを値とする変数のダイアグラム表現、ビット列データ上の演算のダイアグラム表現、変数と演算を組み合わせるためのダイアグラム表現といった所定のダイアグラム表現を使って、ブロック暗号アルゴリズム全体のダイアグラム表現をユーザが記述および編集できる暗号ダイアグラム編集装置が提案されている。また、同文献１には、暗号ダイアグラム編集装置を使って設計されたブロック暗号アルゴリズムからブロック暗号プログラムを自動的に生成する技術や、この生成されたプログラムが元のアルゴリズムを正確に実現しているか否かをテストする技術も提案されている。

【０００５】

他方、本出願人の先願にかかる特開平１１－２１２４５２号公報（以下、文献２と称す）には、開発された暗号プログラムの強度評価を支援する従来技術の一例として、多数の評価データ（平文、鍵等）を使って暗号プログラムの入出力デ

ータのビットごとの相関関係を統計的に求める手段と、求められたビットごとの相関関係を表形式やグラフ形式に編集して出力する手段とを備えた暗号強度評価支援装置が提案されている。

【０００６】

【発明が解決しようとする課題】

文献１に示されるような暗号ダイアグラム編集装置を使えば暗号アルゴリズムの設計を効率化でき、また文献２に示されるような暗号強度評価支援装置を使えば暗号プログラムの強度評価をきめ細かく実施することができる。

【０００７】

しかし、設計された暗号アルゴリズムの強度評価を実施するためには、暗号アルゴリズムから実際の暗号プログラムを生成した後、多数の評価データを使って統計的な処理を実行する必要があり、評価結果が出るまでに多くの時間を要する。１つの暗号アルゴリズムの設計から評価終了までの時間が長大化すると、限られた設計開発期間内で比較検討できる暗号アルゴリズム数、設計変更回数が限定され、利用目的に最適な暗号アルゴリズムを開発することが困難になる。

【０００８】

そこで本発明の目的は、暗号アルゴリズムの評価時間を大幅に短縮し得る暗号評価支援システムを提供することにある。

【０００９】

また本発明の別の目的は、暗号設計の専門家でなくても暗号アルゴリズムの評価を行うことができる暗号評価支援システムを提供することにある。

【００１０】

【課題を解決するための手段】

本発明の暗号評価支援システムは、予め定義した暗号アルゴリズム仕様記述法で記述された暗号アルゴリズムの図形表現を格納する評価対象記憶部と、前記暗号アルゴリズム仕様記述法で使う単位図形の点数を記憶する点数記憶部と、前記評価対象記憶部から図形表現を入力し、該図形表現中の単位図形に対して前記点数記憶部に記憶された点数を付与し、予め定められた計算ルールに従って前記図形表現全体の得点を計算して出力する評価実施手段とを備えている。また、前記

評価実施手段が入力した図形表現中の利用者によって選択された単位図形を他の種類の単位図形に自動的に置き換えた図形表現を生成する自動組み替え手段を備え、前記評価実施手段は、前記入力した図形表現および前記自動組み替え手段で生成された図形表現について得点計算を行う構成も採用している。

【００１１】

暗号アルゴリズムの設計及び評価に関する専門知識を有する技術者は、実際に設計した暗号アルゴリズムの構造と例えば文献２に見られるような暗号強度評価支援装置での評価結果との相関関係など、設計開発に必要な知見を有している。点数記憶部に記憶される各単位図形の点数は、そのような専門技術者の知見に基づいて設定されており、例えば暗号強度に関して良い傾向を持つと判断した単位図形には高い点数を、悪い傾向を持つと判断した単位図形には低い点数が付けられている。ここで、同じ単位図形であっても評価項目（例えばアバランシュ性評価、ビットバランス性評価など）が異なると傾向も異なる場合があるので、点数記憶部には予め定められた複数の評価項目別に単位図形の点数を記憶しておくのが望ましい。また、同じ単位図形であってもビット位置によって傾向も異なる場合があるので、点数はビット単位で設定するのが望ましい。この場合、評価実施手段は、例えば、各評価項目毎に、図形表現中の信号の流れに沿って基本ブロックを通過する毎にその基本ブロックの点数を加点することで、各評価項目毎に、例えば図形表現の各出力ビット毎の得点であるビット得点と、該ビット得点の平均値である項目得点とを算出する。

【００１２】

また本発明の暗号評価支援システムは、前記暗号アルゴリズム仕様記述法による暗号アルゴリズムの図形表現を利用者が記述および編集するのを支援する評価対象編集手段、評価実施手段の計算結果を格納する評価結果記憶部、評価結果記憶部に格納された計算結果をグラフ化して出力する結果編集手段を備えることにより、暗号アルゴリズムの図形表現の編集からその得点計算、グラフ化による比較検討までの一連の作業を１つのシステムで支援可能としている。また、結果編集手段は、評価結果記憶部に格納された計算結果を指定されたソートキーでソートして出力する機能も備えており、複数の暗号アルゴリズムの優劣の判定をより

一層容易にしている。

【００１３】

【発明の実施の形態】

次に本発明の実施の形態の例について図面を参照して詳細に説明する。

【００１４】

図１を参照すると、本発明の一実施の形態にかかる暗号評価支援システム１０は、データ処理装置１１とそれに接続された表示装置１２、入力装置１３および記憶装置１４とを備えている。表示装置１２は例えばＬＣＤであり、入力装置１３は例えばキーボード及びマウスである。記憶装置１４は例えば磁気ディスク装置であり、データ処理装置１１は例えばＭＰＵ及びＲＯＭやＲＡＭ等で構成されたメモリを含むコンピュータ本体である。なお、印刷装置などその他の周辺装置が接続されていても良い。

【００１５】

データ処理装置１１には、予め定義した暗号アルゴリズム仕様記述法による暗号アルゴリズムの図形表現（以下、関数ブロック図と称す）を利用者が記述および編集するのを支援する評価対象編集手段１１１と、関数ブロック図全体の得点を計算する評価実施手段１１２と、計算された得点を編集して出力する結果編集手段１１３とが設けられており、これらはＧＵＩ１１４を通じて表示装置１２および入力装置１３に接続されると共に、記憶インタフェース１１５を通じて記憶装置１４に接続されている。また、関数ブロック図の一部を自動的に変更する自動組み替え手段１１６が評価実施手段１１２および記憶インタフェース１１５に接続されている。なお、本実施の形態では、共通鍵暗号を設計対象とするが、公開鍵暗号への適用も可能である。

【００１６】

他方、記憶装置１４には、評価対象編集手段１１１で編集された関数ブロック図を格納する評価対象記憶部１４１と、暗号アルゴリズム仕様記述法で使う単位図形（以下、単位ブロックと称す）の各評価項目毎の点数を記憶する点数記憶部１４２と、評価実施手段１１２で計算された結果を格納する評価結果記憶部１４３と、自動組み替え手段１１６によって参照される置換部品一覧１４４とが設け

られている。

【００１７】

利用者は、暗号評価支援システム１０を用いて、

（１）関数ブロック図の編集

（２）関数ブロック図の得点計算

（３）計算結果の編集出力

の３つの作業を繰り返しながら、使用目的に合致する暗号アルゴリズムの開発を進めていく。関数ブロック図の編集（１）は暗号アルゴリズムの設計に相当し、主に評価対象編集手段１１１が支援する。関数ブロック図の得点計算（２）は暗号アルゴリズムの評価に相当し、主に評価実施手段１１２が支援する。計算結果の編集出力（３）は関数ブロック図の得点をグラフ化して出力するもので、結果編集手段１１３が支援する。以下、各場合に分けて、本実施の形態のより詳しい構成と動作を説明する。

【００１８】

（１）関数ブロック図の編集

図２は評価対象編集手段１１１の処理例を示すフローチャートである。利用者が入力装置１３から評価対象編集の開始を指示すると、評価対象編集手段１１１が起動され、図２に示す処理が実行される。先ず、評価対象編集手段１１１は、関数ブロック図の新規編集か、過去に作成された関数ブロック図の更新かを、利用者の選択入力に応じて切りわける（Ｓ１１）。更新の場合には、利用者が入力装置１３からファイル名で指定した関数ブロック図を記憶装置１４の評価対象記憶部１４１から読み出し（Ｓ１２）、この読み出した関数ブロック図を初期表示した編集ウィンドウを表示装置１２に表示する（Ｓ１３）。更新でなく新規作成の場合は、関数ブロック図が表示されていない編集ウィンドウを表示装置１２に表示する（Ｓ１３）。その後、利用者からの各種の編集操作に応答して、編集ウィンドウ上で編集処理を実行する（Ｓ１４）。そして、編集作業の終了時、編集された関数ブロック図をファイルとして評価対象記憶部１４１に保存し（Ｓ１５）、評価対象編集手段１１１は処理を終了する。

【００１９】

図３に編集ウィンドウの構成例を示す。この例の編集ウィンドウ２００は、タイトルバー２０１、メニューバー２０２、ツールバー２０３、ステータスバー２０４、関数ブロックウィンドウ３００および基本ブロックバー４００から構成されている。タイトルバー２０１には評価対象編集手段１１１の名前が表示される。メニューバー２０２には、「ファイル」、「編集」、「表示」、「挿入」などのメニュー項目が表示される。メニュー項目をマウスでクリックすると更にドロップダウンメニューが表示され、実行するコマンドを選択することができる。ツールバー２０３にはコマンドを表す一連のボタンが表示される。代表的なコマンドに、切取り、コピー、貼り付け、やり直し等の編集コマンドや、上書保存、新規作成などの他のコマンドがある。ステータスバー２０４にはコマンドの説明やキーボード状態などが表示される。これらはＷｉｎｄｏｗｓ９５等におけるものと同様のものである。

【００２０】

他方、関数ブロックウィンドウ３００は、関数ブロック図を作成するためのウィンドウであり、基本ブロックバー４００は、基本ブロックのボタンを表示する部分である。利用者は、基本ブロックバー４００上のボタンによって適宜に基本ブロックを選択し、関数ブロックウィンドウ３００上の適所に配置していくことで、所望の関数ブロック図を関数ブロックウィンドウ３００上に作成する。

【００２１】

図４は関数ブロックウィンドウ３００の構成例を示す。この例の関数ブロックウィンドウ３００は、タイトルバー３０１、列番号ゲージ３０２、行番号ゲージ３０３、垂直スクロールバー３０４、水平スクロールバー３０５および関数ブロック表示領域３０６から構成されている。関数ブロック表示領域３０６は縦横の枠線によって多数のセルに区切られており、行番号ゲージ３０３にはセルの行番号が、列番号ゲージ３０２にはセルの行番号がそれぞれ表示される。垂直スクロールバー３０４は関数ブロックウィンドウ３００に表示されている部分の垂直位置の調整に使用し、水平スクロールバー３０５は関数ブロックウィンドウ３００に表示されている部分の水平位置の調整に使用する。

【００２２】

関数ブロックウィンドウ３００に表示されている何れかのセルをマウスでクリックすると、そのセルがアクティブセルとなる。図３の基本ブロックバー４００上で基本ブロックのボタンをクリックすると、アクティブセルにその基本ブロックが入力される。既にアクティブセルに基本ブロックが入力されていた場合には新しい基本ブロックで上書きされる。アクティブセルに基本ブロックが入力された時、関数ブロックウィンドウ３００にプロパティウィンドウが開かれ、アクティブセルに入力された基本ブロックの詳細情報が表示される。基本ブロックの詳細情報はプロパティウィンドウにて変更可能である。なお、入力済みの基本ブロックを選択して、そのプロパティウィンドウを開くこともできる。

【００２３】

図５にプロパティウィンドウの構成例を示す。この例のプロパティウィンドウ５００はライン（配線）を分岐する単位ブロックのものであり、その中央部に適用時の当該単位ブロックのイメージ５０１が表示され、その周囲に入出力のデータ幅定義用エデットボックス５０２が配置されている。また、上部には０°、９０°、１８０°、２７０°の４種類の回転ボタン５０３が設けられており、何れかの回転ボタン５０３が操作されると、イメージ５０１がそれに応じて変化する。当該基本ブロックの詳細情報を変更するには、回転ボタン５０３、データ幅定義用エデットボックス５０２で回転角や入出力のデータ幅に変更を加えた後、適用ボタン５０４をクリックする。なお、方向キー代替ボタン５０５はキーボードの方向キーの代替としてアクティブセルの移動に使用される。

【００２４】

図６に基本ブロックバー４００上で選択可能な基本ブロックの一覧を示す。基本ブロックは以下のようなグループに大別される。

（Ａ）接続用（単位ブロック４０１～４１１）

（Ｂ）算術演算用（単位ブロック４１２～４１４）

（Ｃ）論理演算用（単位ブロック４１５～４１７）

（Ｄ）シフト用（単位ブロック４１８～４１９）

（Ｅ）ローテイトシフト用（単位ブロック４２０～４２３）

（Ｆ）その他（単位ブロック４２４～４２７）

【００２５】

接続用の単位ブロックは、更に以下のような種類に分類される。

○ライン；隣接する２つの基本ブロック間を同じデータ幅のラインで接続するための単位ブロックで、単位ブロック４０１～４０３がこれに属する。複数種類用意されているのは、任意の方向での接続を可能にするためである。それらのプロパティウィンドウでは、回転角およびデータ幅が設定可能である。

○フォーク；同じデータ幅で２方向にラインを分岐するための単位ブロックで、単位ブロック４０４、４０５がこれに属する。２種類用意されているのは、任意の方向への分岐を可能にするためである。それらのプロパティウィンドウでは、回転角およびデータ幅が設定可能である。

○クロス；２つのラインが交差する箇所に用いる単位ブロックで、単位ブロック４０６がこれに属する。そのプロパティウィンドウでは、回転角およびデータ幅が設定可能である。

○パーティション；データ幅を分割して２方向にラインを分岐するための単位ブロックで、単位ブロック４０８、４０９がこれに属する。２種類用意されているのは、任意の方向への分岐を可能にするためである。それらのプロパティウィンドウでは、回転角、入力ラインのデータ幅、各出力ライン毎のデータ幅が設定可能である。

○ジョイン；２ラインを１ラインに結合するための単位ブロックで、単位ブロック４１０、４１１がこれに属する。２種類用意されているのは、任意の方向からの結合を可能にするためである。それらのプロパティウィンドウでは、回転角、各入力ライン毎のデータ幅、出力ラインのデータ幅が設定可能である。

【００２６】

算術演算用の単位ブロックとしては、加算用の単位ブロック４１２、減算用の単位ブロック４１３、乗算用の単位ブロック４１４が用意されている。加算と減算の単位ブロック４１２、４１３のプロパティウィンドウでは、回転角およびデータ幅が設定可能である。乗算の単位ブロック４１４のプロパティウィンドウでは、回転角、各入力のデータ幅、出力のデータ幅が設定可能である。

【００２７】

論理演算用の単位ブロックとしては、排他的論理和用の単位ブロック４１５、論理積用の単位ブロック４１６、論理和用の単位ブロック４１７が用意されている。それらのプロパティウィンドウでは、回転角およびデータ幅が設定可能である。

【００２８】

シフト用の単位ブロックとしては、左シフト用の単位ブロック４１８、右シフト用の単位ブロック４１９が用意されている。それらのプロパティウィンドウでは、回転各、データ幅およびシフト量が設定可能である。

【００２９】

ローテイトシフト用の単位ブロックとしては、左ローテイトシフト用の単位ブロック４２０、右ローテイトシフト用の単位ブロック４２１、上入力ダイナミックローテイトシフト用の単位ブロック４２２、下入力ダイナミックローテイトシフト用の単位ブロック４２３が用意されている。単位ブロック４２０、４２１と単位ブロック４２２、４２３の違いは、前者はシフト量が事前に設定された値で固定化されるのに対し、後者は隣接する単位ブロックからのデータがシフト量として入力される点である。左右ローテイトシフトの単位ブロック４２０、４２１のプロパティウィンドウでは、回転角、データ幅およびシフト量が設定可能である。上下入力ダイナミックローテイトシフトの単位ブロック４２２、４２３のプロパティウィンドウでは、回転角、データ幅、シフト量を与えるデータのデータ幅が設定可能である。

【００３０】

その他、複数ビットのデータを他の複数ビットデータに置き換える換字テーブル用の単位ブロック４２４、ビット位置を入れ替える転置テーブル用の単位ブロック４２５、定数用の単位ブロック４２６、鍵用の単位ブロック４２７が用意されている。換字テーブルの単位ブロック４２４のプロパティウィンドウでは、回転角および入出力のデータ幅が設定可能である。転置テーブルの単位ブロック４２５のプロパティウィンドウでは、回転角、入出力のデータ幅および出力ビット位置に対応する入力ビット位置の設定が可能である。鍵と定数の単位ブロックのプロパティウィンドウでは、回転角が設定可能である。なお、本実施の形態にお

ける評価対象編集手段１１１は、暗号アルゴリズム中で実際に使う鍵や定数、転置テーブルの内容を編集する機能は省略しているが、そのような機能を評価対象編集手段１１１に組み込むようにしても良いのは勿論のことである。

【００３１】

利用者は、以上のような基本ブロック４０１～４２７の配置やそのプロパティの調整等を複数回実行することで、関数ブロックウィンドウ３００上に所望の関数ブロック図を作成する。作成した関数ブロック図の一例を図７に示す。入力をｘ、出力をｙとした場合、図７の関数ブロック図は以下の式に対応する。

ｙ＝（ｅ≪ｎ４）◎（ｅ∨ｘ）

ここで、ｅ＝｛（ｄ≪ｎ３）－ｄ｝、ｄ＝｛（ｂ≪ｎ２）◎ｂ｝＋Ｋ、ｂ＝（ａ≪ｎ１）＋Ｃ＋ｘ＋Ｋであり、◎は排他的論理和を、∨は論理和を、≪は左シフトを、ｎ１～ｎ４は図７中に合計４個ある左シフトの単位ブロックのシフト量をそれぞれ示す。

【００３２】

編集を終えた関数ブロック図は、利用者によって指定されたファイル名を付与されて、例えば｛（セルの列番号、行番号）、基本ブロックの詳細情報｝を１レコードとして、評価対象記憶部１４１に保存される。

【００３３】

（２）関数ブロック図の得点計算

図８は評価実施手段１１２の処理例を示すフローチャートである。利用者が入力装置１３から評価実施の開始を指示すると、評価実施手段１１２が起動され、図８に示す処理が実行される。先ず、評価実施手段１１２は、メインダイアログボックスを表示装置１２に表示し（Ｓ２１）、このメインダイアログボックスを通じて利用者から計算対象とする関数ブロック図、評価項目、自動組み替え機能の使用可否等を指定させ、関数ブロック図の読み込み等、必要な事前準備を実行する（Ｓ２２）。

【００３４】

図９にメインダイアログボックスの構成例を示す。この例のメインダイアログボックス６００は、タイトルバー６０１、関数ブロック操作部６０２、評価項目

選択部６０３、結果表示領域６０４および終了ボタン６０５から構成されている。タイトルバー６０１には評価実施手段１１２の名前が表示される。評価項目選択部６０３には、予め定められた幾つかの評価項目を選択するためのボタンＢが表示される。利用者はボタンＢをクリックして評価項目を選択する。評価項目は同時に複数選択可能である。結果表示領域６０４は計算結果を表示する領域であり、終了ボタン６０５は評価実施の終了を指示するボタンである。

【００３５】

関数ブロック操作部６０２には、評価を実施する関数ブロック図のファイル名を入力するエデットボックス６０６がある。利用者は入力装置１３から直接にファイル名をエデットボックス６０６に入力できる他、参照ボタン６０７をクリックすれば評価対象記憶部１４１に保存されている関数ブロック図のファイル名の一覧が表示されるので、その中から選択して入力することも可能である。ファイル名の入力後に関数読み込みボタン６０８がクリックされると、評価実施手段１１２は評価対象記憶部１４１から該当する関数ブロック図を内部に読み込む。

【００３６】

また関数ブロック操作部６０２には、自動組み替え機能のオン、オフボタン６０９があり、利用者が何れか一方を選択できるようになっている。自動組み替え機能をオンした場合、評価実施手段１１２は、エデットボックス６０６でファイル名が指定された関数ブロック図を図４の関数ブロックウィンドウと同様なウィンドウに展開した試行マス選択ウィンドウを表示装置１２に表示し、利用者にその画面上で試行マスを選択させる。試行マスとは、自動組み替え対象となる単位ブロックが配置されているセルのことである。試行マスの選択は、置換元となる単位ブロックが配置されているセルを例えばクリックすることで可能である。評価実施手段１１２は、選択された試行マスに配置されている単位ブロックが他の単位ブロックに置き換え可能な単位ブロックであれば、その試行マスの選択を有効とし、他のブロックに置き換え不可能な単位ブロックであれば、その旨表示して利用者に他のセルの選択を促す。他の基本ブロックに置き換え可能か否かは、選択された試行マスに配置されている単位ブロックの種類をキーに置換部品一覧１４４を検索し、置き換え可能な単位ブロックが少なくとも１つ以上設定されて

いるか否かによって判断する。

【００３７】

更に関数ブロック操作部６０２には、計算の実行開始を指示する計算実行ボタン６１０、計算結果を保存するファイル名を入力するエデットボックス６１１、その参照ボタン６１２と結果保存ボタン６１３とが設けられている。利用者は入力装置１３から直接にファイル名をエデットボックス６１１に入力できる他、参照ボタン６１２をクリックすれば評価結果記憶部１４３に保存されている評価結果ファイル名の一覧が表示されるので、その中から選択して入力することも可能である。ファイル名の入力後に結果保存ボタン６１３がクリックされると、評価実施手段１１２は計算結果を該当するファイルに保存する。

【００３８】

評価実施手段１１２は、評価対象とする関数ブロック図の読み込み、自動組み替え機能のオン、オフの設定および評価項目の選択が完了した後、計算実行ボタン６１０がクリックされると、自動組み替え機能がオンの場合とオフの場合とで処理を切りわける（図８のＳ２３）。以下、各場合に分けて説明する。

【００３９】

○自動組み替え機能オフの場合

評価実施手段１１２は、選択された評価項目の１つに注目し（Ｓ２４）、点数記憶部１４２中の当該評価項目にかかる各単位図形の点数を参照して、評価対象とする関数ブロック図の当該評価項目にかかる得点を計算する（Ｓ２５）。得点の計算方法については後述する。１つの評価項目の得点を計算すると、選択された評価項目の残りの１つに注目を移し（Ｓ２６、Ｓ２７）、同様の処理を繰り返す。以下、選択された全ての評価項目について、評価対象関数ブロック図の得点を計算する。

【００４０】

○自動組み替え機能オンの場合

評価実施手段１１２は、評価対象とする関数ブロック図と試行マスの情報とを自動組み替え手段１１６に渡し、関数ブロック図の自動組み替えを実行させる（Ｓ２８）。図１０に自動組み替え手段１１６の処理例を示す。自動組み替え手段

１１６は、評価実施手段１１２から関数ブロック図と試行マスの情報とを入力すると（Ｓ５１）、関数ブロック図上の試行マスに配置されている単位ブロックを識別し、その単位ブロックの種類をキーに置換部品一覧１４４を検索して、その単位ブロックと置換可能な単位ブロックを決定する（Ｓ５２）。

【００４１】

置換部品一覧１４４の一例を図１１に示す。置換部品一覧１４４には、置き換え元となり得る単位ブロック毎に、置き換え可能な基本ブロックが記述されている。図１１の場合、加算、減算、排他的論理和、論理積、論理和の基本ブロック４１２、４１３、４１５、４１６、４１７は相互に置換可能に指定されている。また左右シフトの単位ブロック４１８、４１９間、左右ローテイトシフトの単位ブロック４２０、４２１間、換字テーブル単位ブロック４２４と転置テーブル単位ブロック４２５間がそれぞれ置換可能に指定されている。

【００４２】

自動組み替え手段１１６は、置換可能な単位ブロックを決定すると、関数ブロック図中の試行マスの単位ブロックを前記決定した単位ブロックで置き換えることにより、置換可能な単位ブロック毎の関数ブロック図を生成する（Ｓ５３）。そして、生成した関数ブロック図を評価実施手段１１２に出力する（Ｓ５４）。

【００４３】

評価実施手段１１２は、自動組み替えが完了すると、利用者が評価対象として指定した関数ブロック図及び自動組み替え手段１１６で生成された関数ブロック図を評価対象関数ブロック図群とし、先ずその１つの関数ブロック図に注目する（Ｓ２９）。次いで、ステップＳ２４～Ｓ２７と同様なステップＳ３０～Ｓ３３を実行することにより、当該関数ブロック図の各評価項目毎の得点を計算する。１つの関数ブロック図についての得点計算が終了すると（Ｓ３３でＹＥＳ）、評価対象関数ブロック図群の残り関数ブロック図の１つに注目を移し（Ｓ３４）、その関数ブロック図の各評価項目毎の得点を計算する（Ｓ３０～Ｓ３３）。以下同様にして、評価対象関数ブロック図群の残りの関数ブロック図についても各評価項目毎の得点を計算する。

【００４４】

以上のようにして関数ブロック図の得点計算が終了すると（Ｓ２７またはＳ３５でＹＥＳ）、評価実施手段１１２は、計算結果を結果表示領域６０４に表示する（Ｓ３６）。利用者は計算結果を保存する場合、前述したように結果ファイル名を指定して結果保存ボタン６１３をクリックすれば、計算結果が評価結果記憶部１４３に格納される（Ｓ３７、Ｓ３８）。なお、自動組み替え手段１１６がオンの場合、自動組み替え手段１１６で自動生成された関数ブロック図が、例えば生成元の関数ブロック図のファイル名の後ろに連番を付したファイル名で、評価対象記憶部１４１に自動的に格納される。

【００４５】

次に関数ブロック図の得点計算について、基本ブロックの点数と得点計算方法とに分けて説明する。

【００４６】

○基本ブロックの点数

点数記憶部１４２には、図１２に示すように、各評価項目Ａ、Ｂ、…、Ｎ毎に基本ブロックの点数がビット単位で設定されている。評価項目Ａ、Ｂ、…、Ｎは、具体的には、アバランシュ性評価、入出力間関連性評価、出力ビット間関連性評価、ビットバランス性評価などの強度評価項目である。

【００４７】

ここで、アバランシュ性評価とは、入力データに１ビットの変化を与えたときに出力ビットにどれだけ波及するかを評価するもので、入力の反転場所と出力の反転場所に有為な関係が存在せず、入力の反転ビット数と出力の反転ビット数に有為な関係が存在しない程、評価が高い。

【００４８】

入出力ビット間関連性評価とは、入力データの各ビットと出力データの各ビットとの関連性を評価するもので、入力ビット値と有為な関係を持つ出力ビット値が存在しない程、評価が高い。

【００４９】

出力ビット間関連性評価とは、出力データの各ビット間の関連性を評価するもので、どの出力ビット値どうしも有為な関係が存在しない程、評価が高い。

【００５０】

ビットバランス性評価とは、出力データの各ビットごとの１、０の出現頻度を評価するもので、入力値に依らずにどの出力ビットも０、１の出現比が１対１に近い程、評価が高い。

【００５１】

点数記憶部１４２において評価項目別に点数が設定されている理由は、同じ基本ブロックであっても評価項目が相違すれば暗号強度に及ぼす影響が異なる場合があり、その場合に付与する点数を相違させなければならないためである。例えば、論理和や論理積の基本ブロックは、ビットバランス性評価に関しては強度を弱める方向に作用することがあるが、出力ビット関連性評価に関しては強度変化に影響を与えず、アバランシュ性評価に関しては強度を強める方向に作用する。

【００５２】

また点数記憶部１４２において基本ブロックの点数をビット単位で設定する理由は、同じ基本ブロックであってもビット位置によって強度変化に及ぼす影響が異なる場合があるためである。例えば、アバランシュ性評価において、加算や減算の単位ブロックは、自出力ビット番号より下位の入力ビットが反転した場合、有為な関係が存在しないために強度を強めるように作用するので、自出力ビット番号より下位に入力ビットを持たない最下位１ビットとそれ以外のビットとは強度変化に及ぼす影響が相違する。

【００５３】

基本ブロックの各ビット毎の点数は、例えば、強度に変化が無い場合を０点とし、強くしている場合は正数、弱くしている場合は負数を与える。絶対値が大きいほどその度合いが大きいことを表す。具体的な点数の設定は、各評価項目毎に、基本ブロック間および基本ブロック内のビット間で比較し、評価経験に関する専門知識を有する者が当該評価項目に関して良い傾向を持つと判断したものには高い点数を、悪い傾向のものには低い点数を定義することで行う。なお、必ずしも全ての基本ブロックに点数を定義する必要はない。例えば、鍵や定数の基本ブロックへの点数の付与は省略できる。点数が定義されていない基本ブロックでは後述する加点はない。

【００５４】

○得点の計算方法

ビット単位で持ち点を加点する。原則として入力ビットの得点（入力が複数ある場合はその総和）に、通過する基本ブロックの点数を加点する。単位ブロックの種類毎の加点方法の具体例を以下に示す。

【００５５】

（ａ）接続

（入力ビットの得点＋点数）

（ｂ）加算、減算、論理和、論理積、排他的論理和

（同一入力ビット番号同士の得点の総和＋点数）

（ｃ）乗算

（同一入力ビット番号同士の得点の総和を２倍の幅に広げたもの＋点数）

ここで、２倍の幅に広げたものとは、同一入力ビット番号同士の得点の総和を、例えばｘ１，ｘ２，ｘ３，ｘ４（４ビットの場合）とすると、ｘ１，ｘ１，ｘ２，ｘ２，ｘ３，ｘ３，ｘ４，ｘ４である。

（ｄ）シフト

（入力ビットの得点＋点数）をシフト数に従って移動し、空いた出力ビットには０点を設定する。

（ｅ）ローテイトシフト

（入力ビットの得点＋点数）をシフト数に従って移動する。

（ｆ）ダイナミックローテイトシフト

（入力ビットの最小点＋シフトの最小点＋点数）を計算し、全出力ビットの得点を置き換える。

（ｇ）換字

（入力ビットの得点＋点数）を計算し、計算結果の最小点で全出力ビットの得点を置き換える。

（ｈ）転置

転置テーブルが定義されているときは、複数回出現するビットについては出現回数に応じて（入力ビットの得点＋点数）を計算し、１回しか出現しないビット

についてはそのままでテーブルに従って移動する。転置テーブルが定義されていないときは、（入力ビットの得点＋点数）を計算し、計算結果の最小点で全出力ビットの得点を置き換える。

【００５６】

例えば、入力ビットａ０～ａ３１と入力ビットｂ０～ｂ３１とを入力し、各ビット毎の論理和をとって出力ビットｃ０～ｃ３１を生成する論理和の基本ブロックにおいて、当該基本ブロックのビット番号０の点数を「１」、入力ビットａ０の得点を「３」、入力ビットｂ０の得点を「５」とした場合、出力ビットｃ０の得点は、３＋５＋１＝９となる。この出力ビットｃ０が次の基本ブロックの入力ビットｄ０となる場合、その入力ビットｄ０は「９」の得点を持つものとして扱われる。

【００５７】

このように本実施の形態において、基本ブロックを通過する毎に持ち点を順次加算していく加点方式を採用したのは、計算が簡易であり、関数ブロック図１つ当たりの計算時間を短くするためである。勿論、本発明はこのような計算方法に限定されるものではない。

【００５８】

さて、以上のような計算方法により、本実施の形態では、１つの関数ブロック図について、各評価項目ごとに以下のような得点が計算される。

（ａ）ビット得点；関数ブロック図の出力における各出力ビットごとの得点。

（ｂ）項目得点；ビット得点の平均値。

（ｃ）関数ブロック得点；項目得点の総和。

ビット得点と項目得点は図８のステップＳ２５、Ｓ３１で計算され、関数ブロック得点はステップＳ３６の計算結果の表示時に計算される。

【００５９】

（３）計算結果の編集出力

図１３は結果編集手段１１３の処理例を示すフローチャートである。利用者が入力装置１３から結果編集出力の開始を指示すると、結果編集手段１１３が起動され、図１３に示す処理が開始される。結果編集手段１１３は、先ず、評価結果

記憶部１４３に格納された一連の結果ファイル群の中から編集出力したい結果ファイルを利用者に選択させる（Ｓ６１）。これはファイル名を利用者に直接入力させても良く、ファイル名一覧を表示装置１２に表示して選択させるようにしても良い。１つのファイルだけを選択することもでき、複数のファイルを選択することもできる。複数のファイルを選択した場合、同一グラフ上に複数の関数ブロック図の得点が表示されることになる。

【００６０】

次に結果編集手段１１３は、得点種別を利用者に選択させる（Ｓ６２）。ここで、得点種別には、ビット得点、項目得点がある。ビット得点を選択した場合、評価項目も併せて選択させる。

【００６１】

次に結果編集手段１１３は、グラフ形式を利用者に選択させる（Ｓ６３）。これは、例えばグラフ形式の一覧を表示装置１２に表示し、その中から利用者に所望のものを選択させるようにして良い。グラフ形式には、レーダーチャート、折れ線グラフ等の複数の形式が用意されている。

【００６２】

結果ファイル及びグラフ形式が決定すると、結果編集手段１１３は、該当する結果ファイルを評価結果記憶部１４３から読み込み、決定したグラフ形式のグラフを作成し（Ｓ６４）、表示装置１２に表示する（Ｓ６５）。印刷装置がある場合、プリントアウトさせることも可能である。

【００６３】

図１４および図１５に表示装置１２に表示されるグラフの例を示す。図１４では、複数の関数ブロック図Ｘ、Ｙ、Ｚの各評価項目Ａ、Ｂ、…、毎の項目得点がレーダーチャート形式で表示されている。一般に面積が大きくなるほど良い傾向となるので、複数の関数ブロック図の比較を容易に行うことができる。また、個々の関数ブロック図についても評価項目どうしの関連を調べることによって、設計した暗号アルゴリズムの良否を判断できる。

【００６４】

図１５は複数の関数ブロック図Ｘ、Ｙ、Ｚの或る評価項目Ａについての出力ビ

ット毎の得点が折れ線グラフ形式で表示されている。横軸が出力ビット、縦軸がビット得点である。一般にグラフが上方向に推移するほど良い傾向となるので、複数の関数ブロック図の比較を容易に行うことができる。また、個々の関数ブロック図についても、出力ビットどうしの関連を調べることによって、設計した暗号アルゴリズムの良否を判断できる。

【００６５】

また、本実施の形態の結果編集手段１１３は、複数の関数ブロック図をその得点によってソートする機能も有している。図１６にその処理例を示す。利用者が入力装置１３からソートの開始を指示すると、結果編集手段１１３が起動され、図１６に示す処理が開始される。結果編集手段１１３は、先ず、評価結果記憶部１４３に格納された一連の結果ファイル群の中からソートしたい複数の結果ファイルを利用者に選択させる（Ｓ７１）。これはファイル名を利用者に直接入力させても良く、ファイル名一覧を表示装置１２に表示して選択させるようにしても良い。

【００６６】

次に結果編集手段１１３は、ソートキーに使う評価項目を利用者に選択させる（Ｓ７２）。ソートキーは、第１ソートキーから第ｍソートキーまで最大ｍレベル指定でき、利用者は暗号の用途などの設計要件に応じてソートキーの数と各レベル毎の評価項目を選択する。各レベルのソートキーとしてどの評価項目を使うかを外部ファイルに設定しておくことも可能であり、その場合は外部ファイルを選択すれば良い。

【００６７】

結果ファイル及びソートキーが決定すると、結果編集手段１３は、該当する結果ファイルを評価結果記憶部１４３から読み込み、より上位レベルのソートキーで指定された評価項目の得点（項目得点）が高くなる順序に結果ファイルを並べ替え（Ｓ７３）、順位の高い順に結果ファイル名を並べたソート結果を表示装置１２に表示する（Ｓ７４）。印刷装置がある場合、プリントアウトさせることも可能である。

【００６８】

以上のようなソート機能を使えば、例えば自動組み替え機能を使って或る単位ブロックを別の単位ブロックに置き換えて生成した複数の関数ブロック図（生成元の関数ブロック図を含む）の結果ファイルを選択し、得点計算時に指定した各評価項目をソートキーに指定したソートを行うことで、複数の関数ブロック図の優劣を容易に判断することが可能となる。勿論、自動組み替え機能で生成された関数ブロック図以外の複数の関数ブロック図のソートも可能である。

【００６９】

図１７は本発明を適用したコンピュータの構成例を示す平面図である。コンピュータ１は、中央処理装置、主記憶等のメモリ、ハードディスク装置、フロッピィディスク装置、ＣＤ－ＲＯＭユニットなどを備えるコンピュータ本体２と、表示装置３と、キーボード４と、マウス５とで構成される。６はフロッピィディスク、ＣＤ－ＲＯＭ等の機械読み取り可能な記録媒体であり、暗号評価支援プログラムが記録されている。記録媒体６に記録された暗号評価支援プログラムは、コンピュータ本体２によって読み取られ、コンピュータ本体２の動作を制御することにより、コンピュータ本体２のメモリに評価対象記憶部１４１、点数記憶部１４２、評価結果記憶部１４３および置換部品一覧１４４をロードすると共に、コンピュータ本体２上に、評価対象編集手段１１１、評価実施手段１１２、結果編集手段１１３、ＧＵＩ１１４、記憶インタフェース１１５および自動組み替え手段１１６を生成する。

【００７０】

以上本発明の実施の形態について説明したが、本発明は以上の実施形態にのみ限定されず、その他各種の付加変更が可能である。例えば評価項目としては主に統計的な暗号強度に関する評価項目を例示したが、線形解読法など攻撃に対する暗号強度に関する評価項目も同じ原理で適用可能である。また、設計した暗号アルゴリズムをソフトウェアやハードウェアで実行した場合の処理量や規模の見積もりにも同じ原理で適用可能である。また、複数の基本ブロックをユーティリティブロックとして、あたかも１つの基本ブロックのように扱えるマクロ機能を評価対象編集手段１１１に持たせるようにしても良い。

【００７１】

【発明の効果】

以上説明したように本発明によれば以下のような効果が得られる。

【００７２】

暗号アルゴリズムの評価時間を大幅に短縮することができる。その理由は、文献２に記載の暗号強度評価支援装置のように実際の暗号プログラムを用いた統計的な処理が不要であり、暗号アルゴリズムの図形表現の段階で得点計算という非統計的な処理で評価結果が得られるためである。但し、本発明の暗号評価支援システムによる評価結果は文献２に記載の暗号強度評価支援装置による評価結果よりも正確さで劣るため、数多く設計した暗号アルゴリズムを先ず本発明の暗号評価支援システムで選別し、上位幾つかの暗号アルゴリズムを文献２記載の暗号強度評価支援装置などを使ってより正確に評価することが必要である。

【００７３】

暗号設計の専門家でなくても暗号アルゴリズムの評価を行うことができる。その理由は、得点という数値によって優劣を判断できるためである。また、複数の暗号アルゴリズムの優劣を得点の大小で判断できるためである。

【００７４】

自動組み替え手段を持つ構成にあっては、多くの暗号アルゴリズムの設計と評価を効率良く実施することができる。その理由は、指定した図形単位を他の図形単位に置き換えた図形表現が自動的に作成されるからである。

【００７５】

グラフ化機能を持つ結果編集手段を備えた構成にあっては、得点をグラフ化できるため優劣を直感的に把握でき、またソート機能を持つ結果編集手段を備えた構成にあっては、複数の暗号アルゴリズムを自動的に順序付けることができる。

【図面の簡単な説明】

【図１】

本発明の一実施の形態にかかる暗号評価支援システムのブロック図である。

【図２】

評価対象編集手段の処理例を示すフローチャートである。

【図３】

編集ウィンドウの構成例を示す図である。

【図４】

関数ブロックウィンドウの構成例を示す図である。

【図５】

プロパティウィンドウの構成例を示す図である。

【図６】

基本ブロックバー上で選択可能な基本ブロックの一覧を示す図である。

【図７】

関数ブロック図の一例を示す図である。

【図８】

評価実施手段の処理例を示すフローチャートである。

【図９】

メインダイアログボックスの構成例を示す図である。

【図１０】

自動組み替え手段の処理例を示すフローチャートである。

【図１１】

置換部品一覧の一例を示す図である。

【図１２】

点数記憶部の構成例を示す図である。

【図１３】

結果編集手段の処理例を示すフローチャートである。

【図１４】

表示装置に表示されるグラフの例を示す図である。

【図１５】

表示装置に表示されるグラフの他の例を示す図である。

【図１６】

結果編集手段の他の処理例を示すフローチャートである。

【図１７】

本発明を適用したコンピュータの構成例を示す平面図である。

【符号の説明】

１０…暗号評価支援システム

１１…データ処理装置

１１１…評価対象編集手段

１１２…評価実施手段

１１３…結果編集手段

１１４…ＧＵＩ

１１５…記憶インタフェース

１１６…自動組み替え手段

１２…表示装置

１３…入力装置

１４…記憶装置

１４１…評価対象記憶部

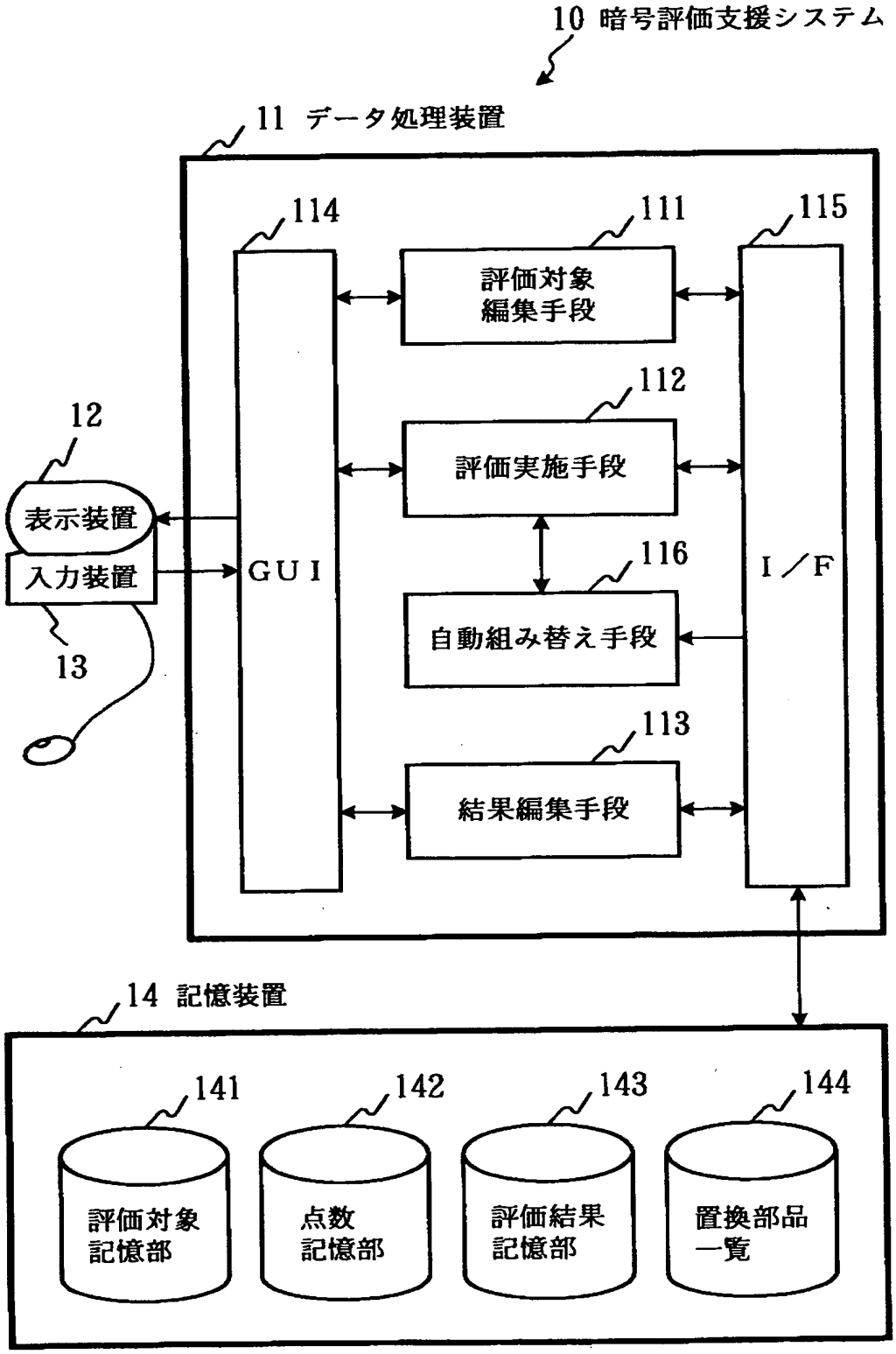
１４２…点数記憶部

１４３…評価結果記憶部

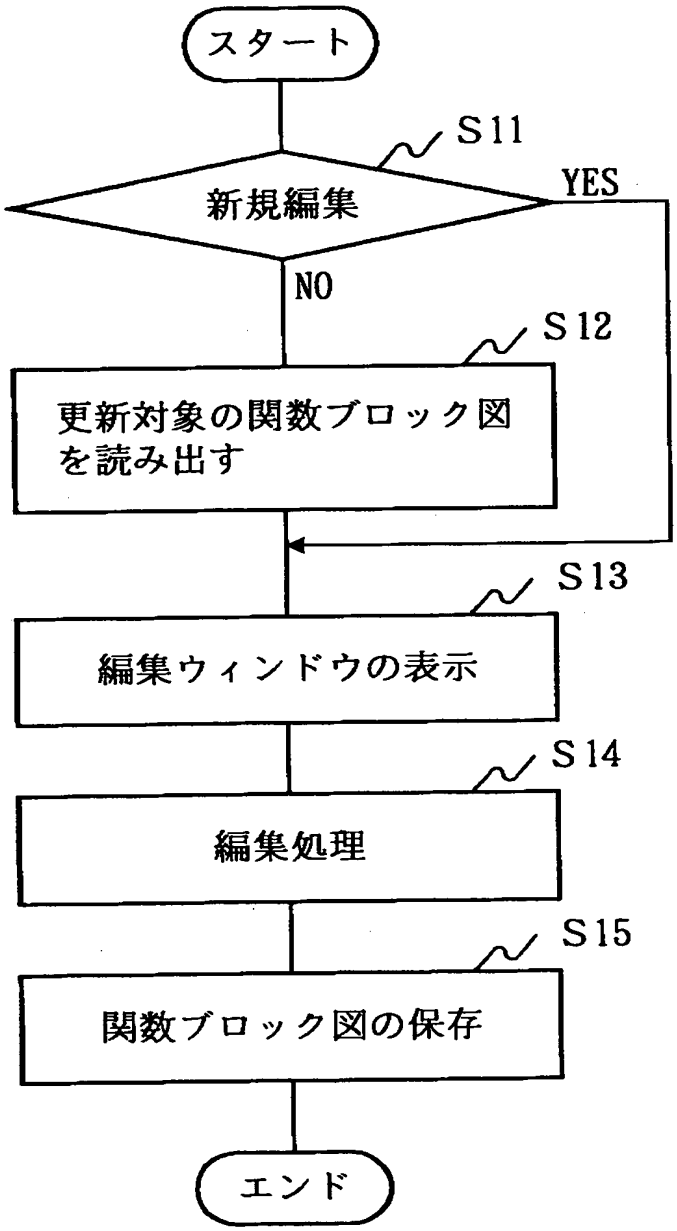
１４４…置換部品一覧

【書類名】　　図面

【図１】

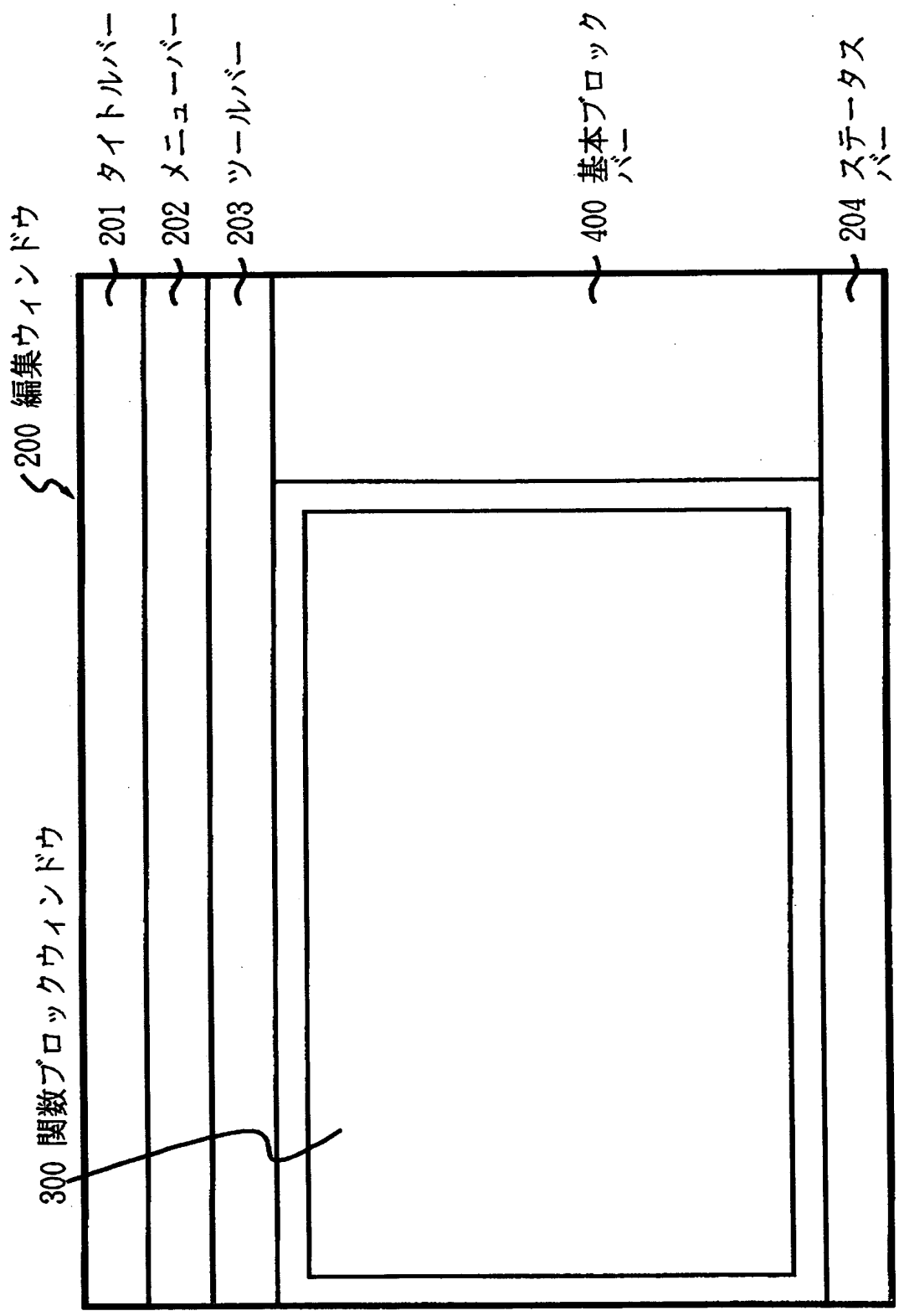

10 暗号評価支援システム
11 データ処理装置
114
111
115
評価対象
編集手段
112
12
評価実施手段
表示装置
入力装置
GUI
116
I／F
13
自動組み替え手段
113
結果編集手段
14 記憶装置
141
142
143
144
評価対象
記憶部
点数
記憶部
評価結果
記憶部
置換部品
一覧

【図２】



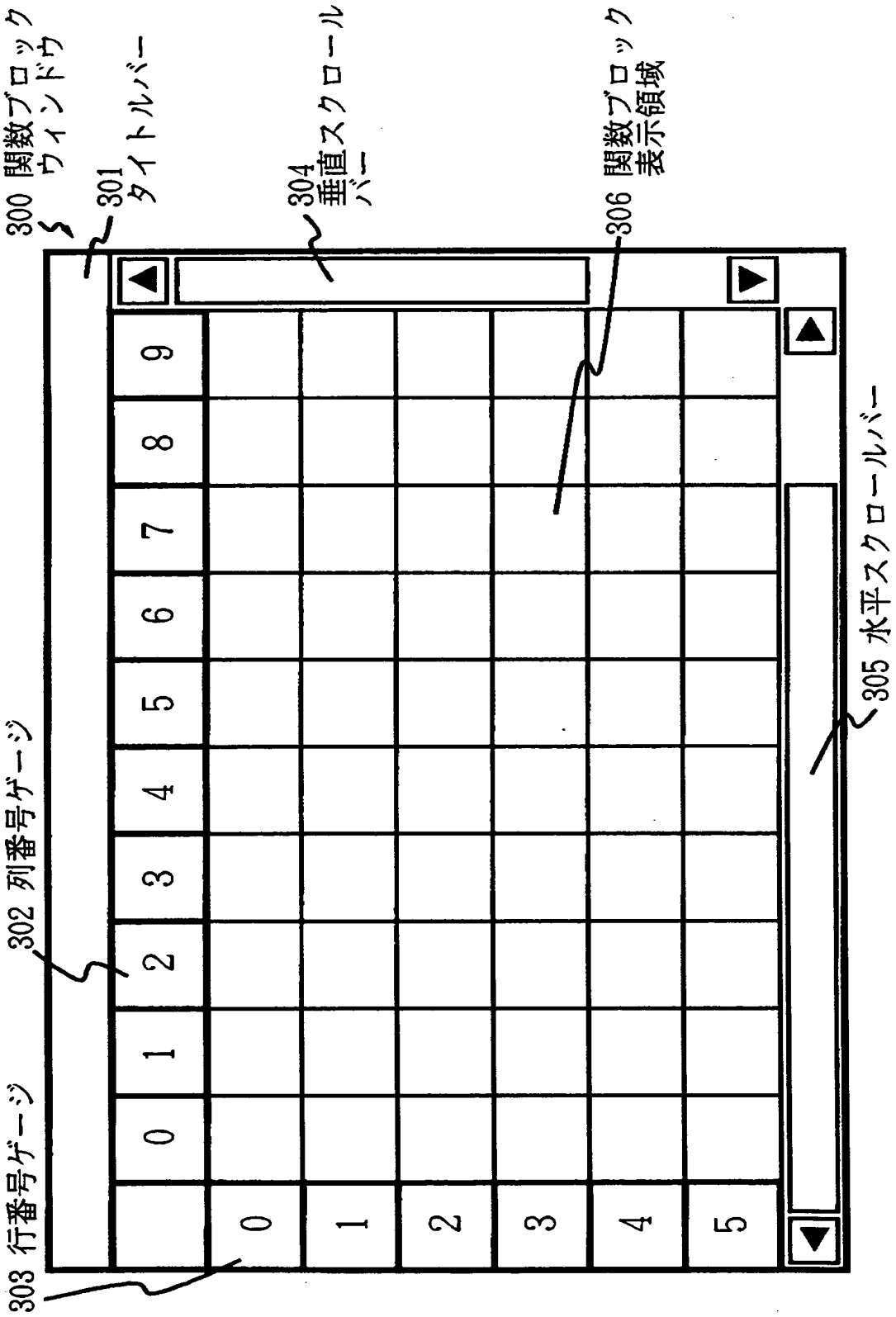
出証特２０００－３０８４３９９

【図３】

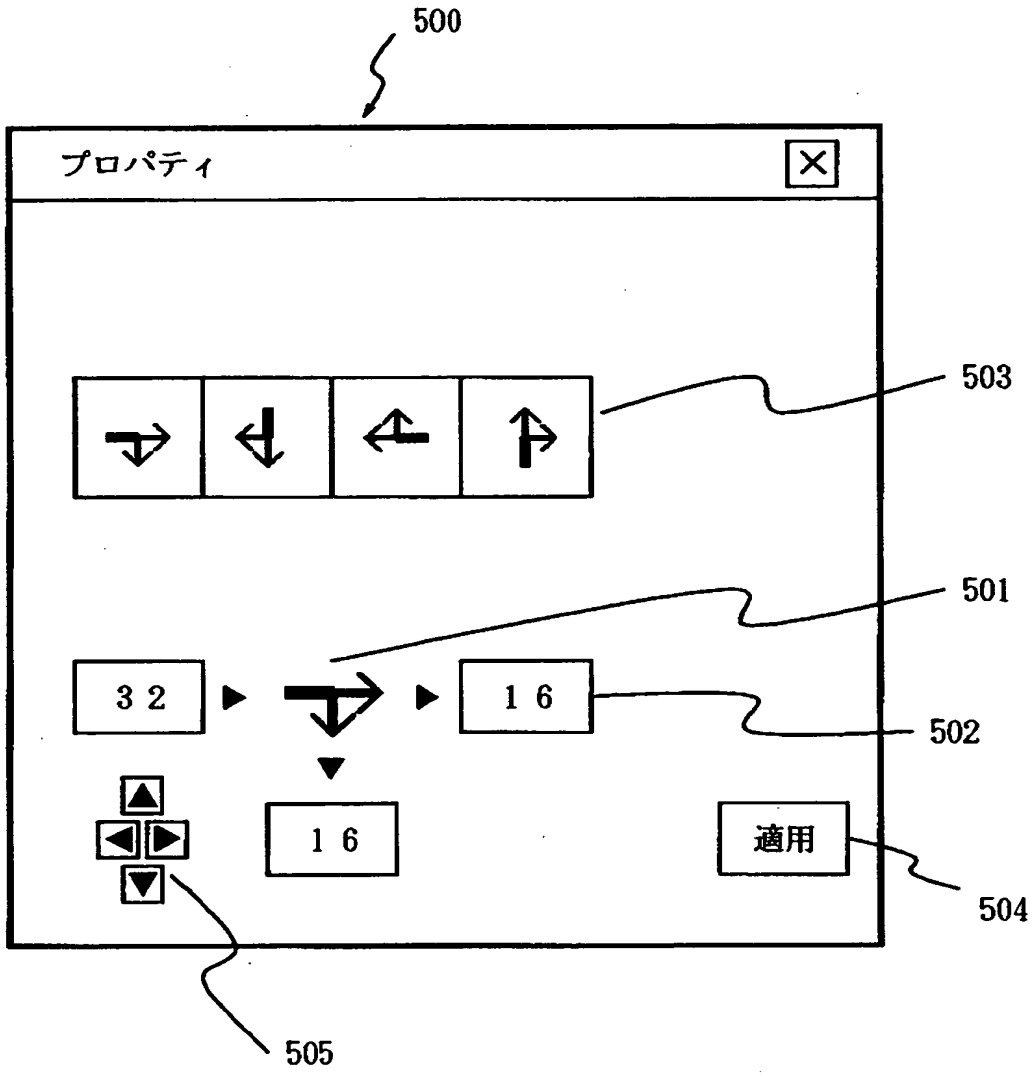


出証特２０００－３０８４３９９

【図４】

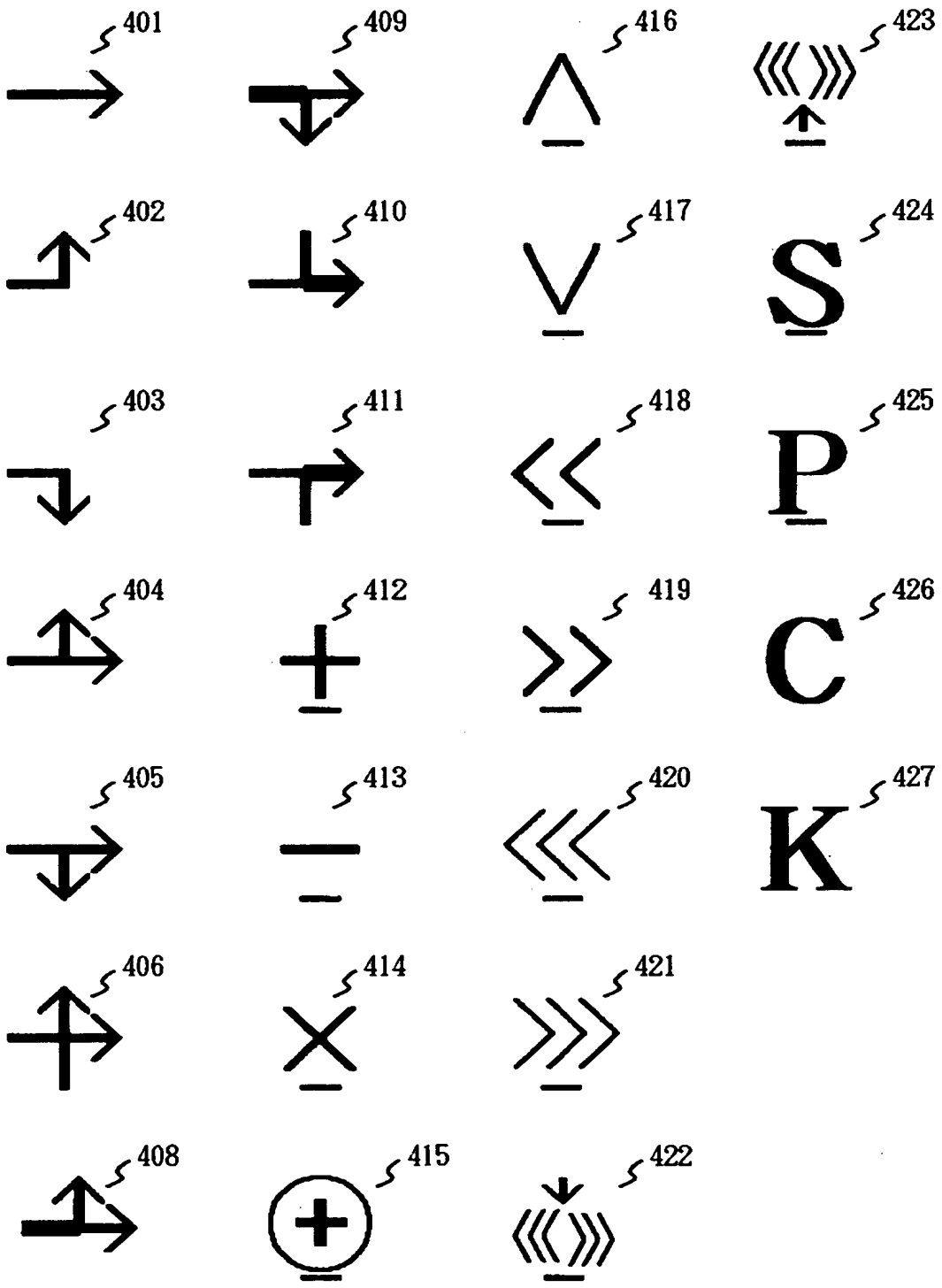

300 関数ブロック ウィンドウ
301 タイトルバー
304 垂直スクロール バー
306 関数ブロック 表示領域
305 水平スクロールバー
302 列番号ゲージ
303 行番号ゲージ
0
1
2
3
4
5
6
7
8
9

【図５】

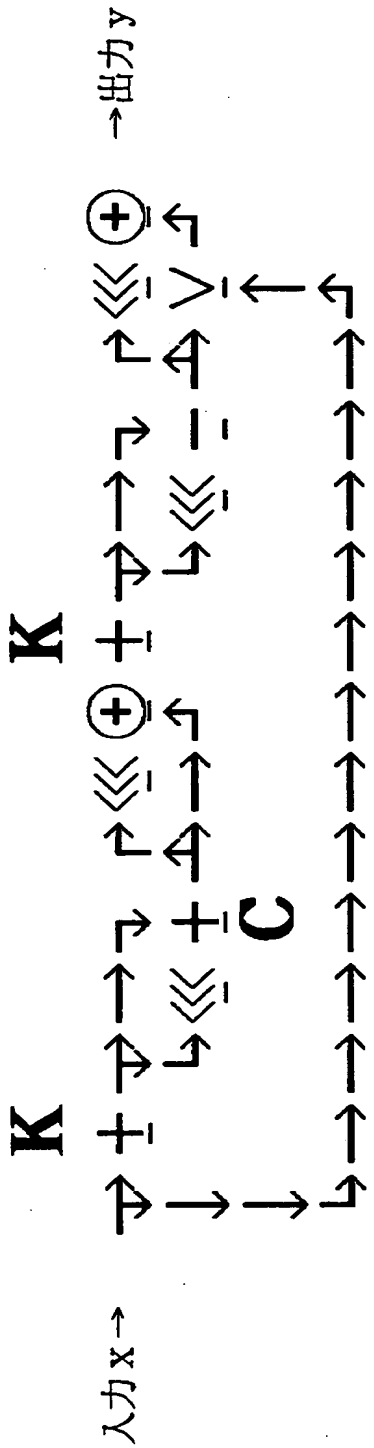


出証特２０００－３０８４３９９

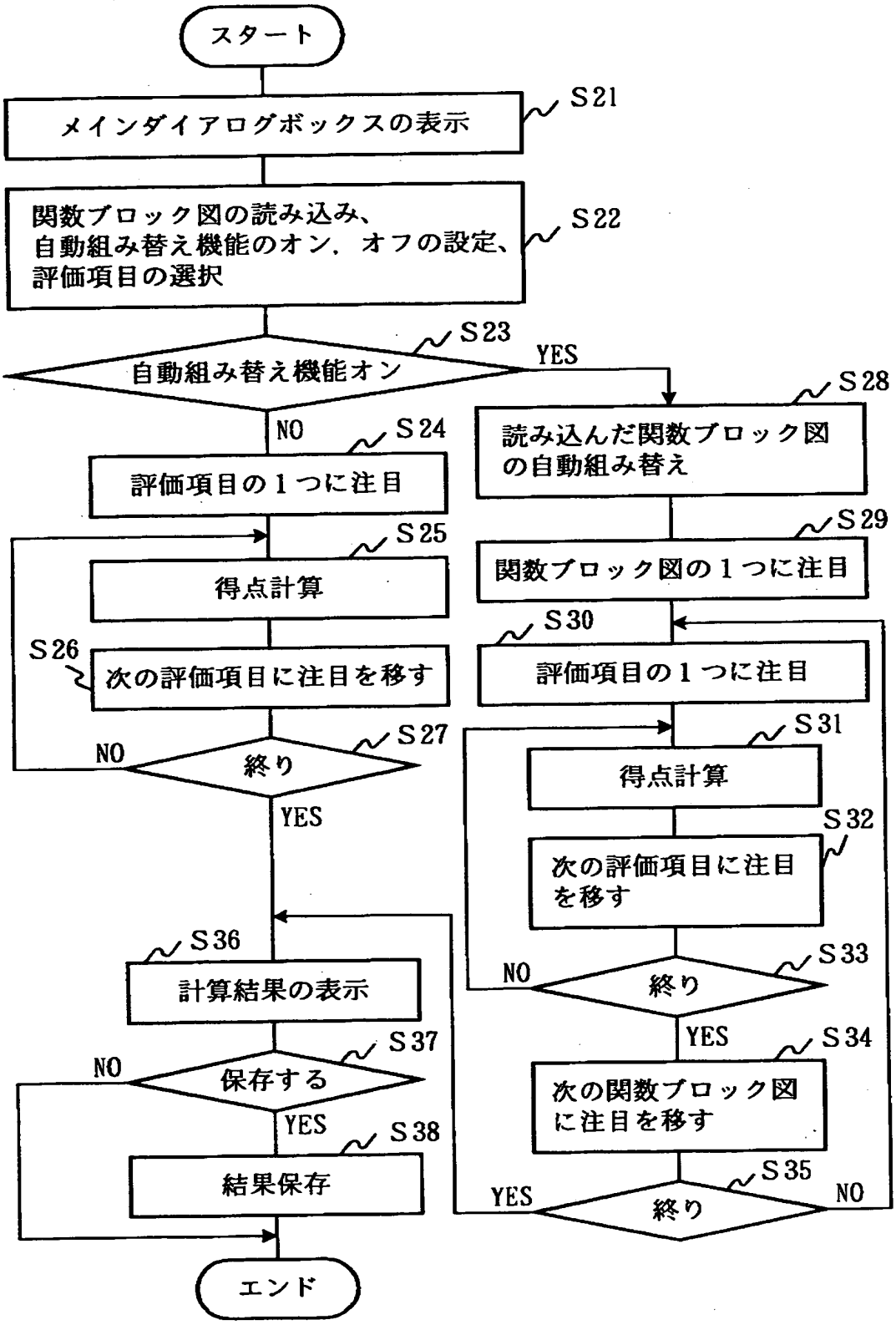
【図６】


401
409
416
423
402
410
417
424
S
403
411
418
425
P
404
412
419
426
C
405
413
420
427
K
406
414
421
408
415
422

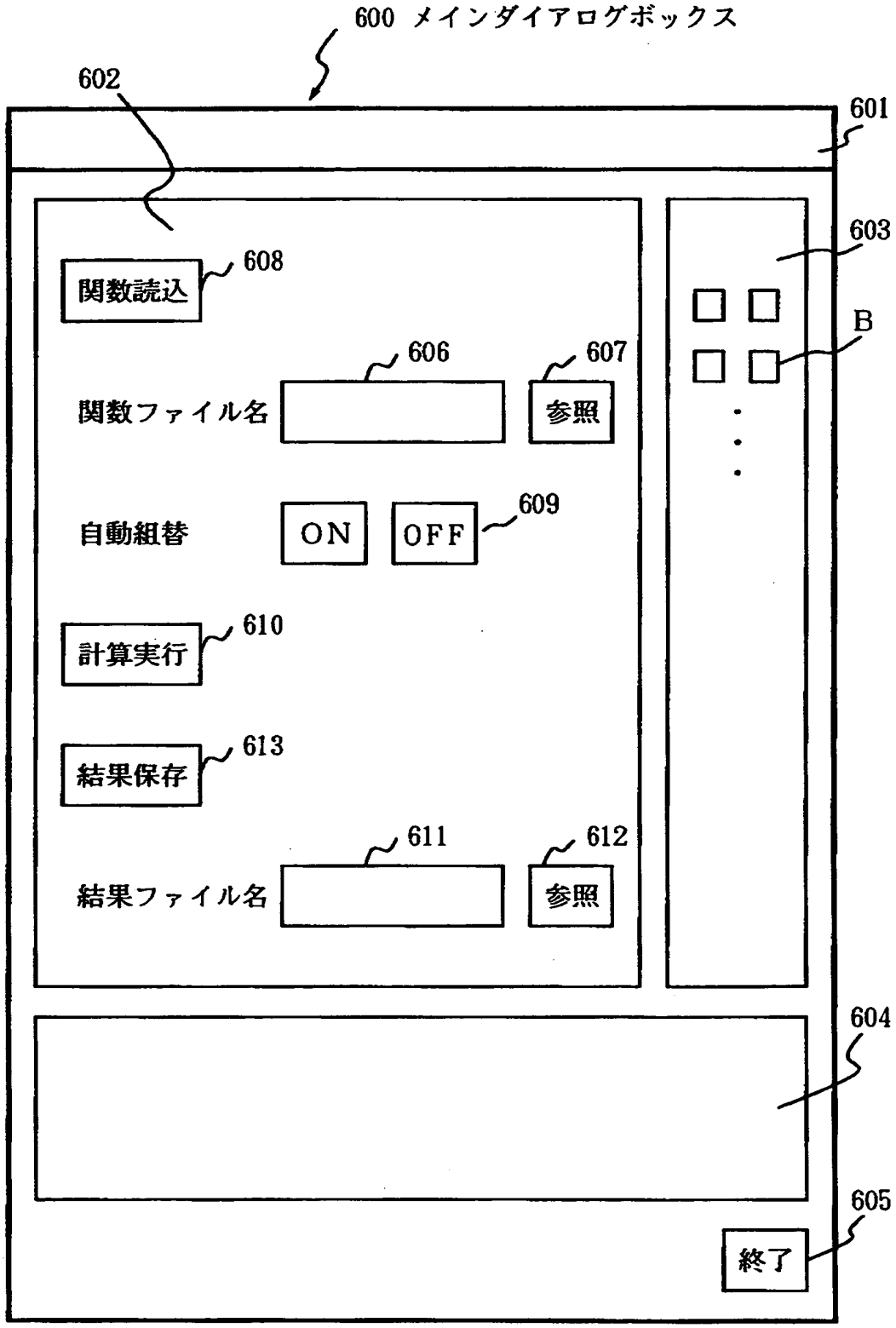
【図７】



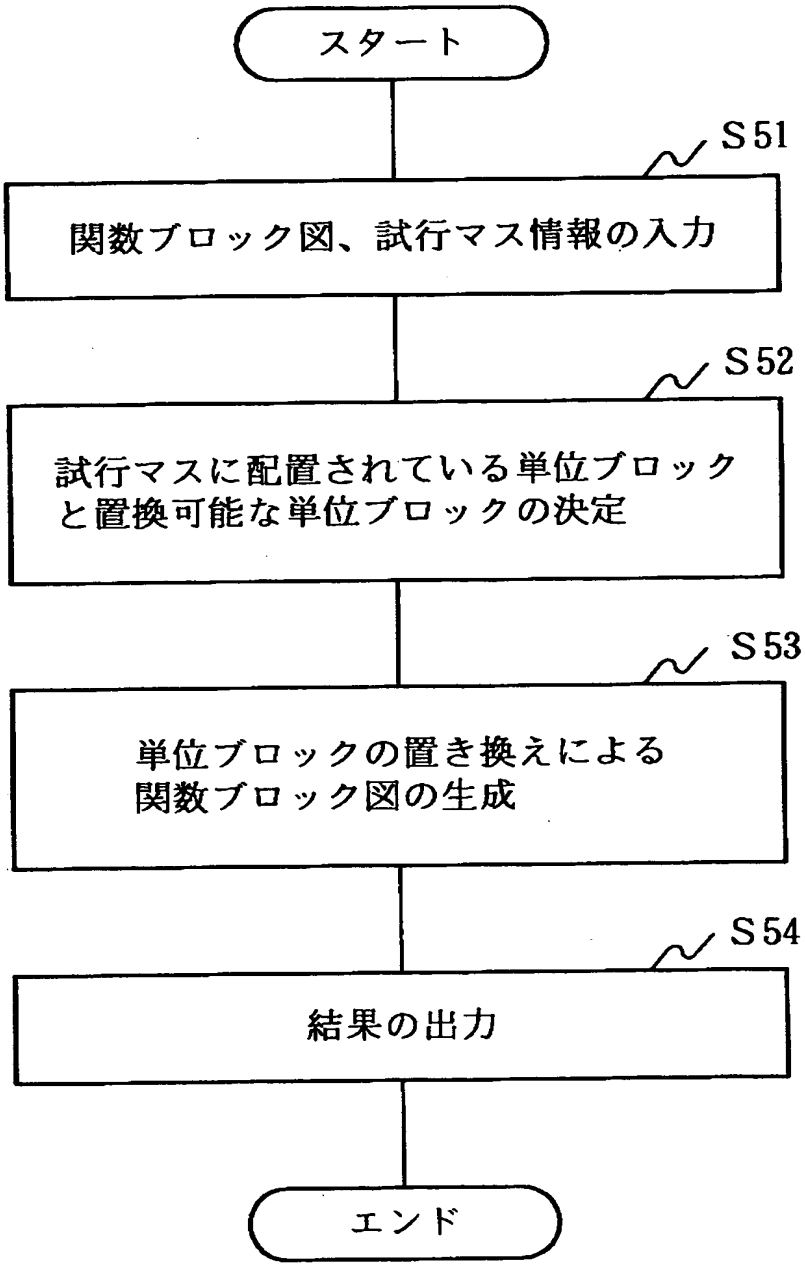
【図８】


スタート
メインダイアログボックスの表示
S21
関数ブロック図の読み込み、
自動組み替え機能のオン．オフの設定、
評価項目の選択
S22
S23
自動組み替え機能オン
YES
NO
S24
評価項目の１つに注目
S25
得点計算
S26
次の評価項目に注目を移す
S27
NO
終り
YES
S28
読み込んだ関数ブロック図
の自動組み替え
S29
関数ブロック図の１つに注目
S30
評価項目の１つに注目
S31
得点計算
S32
次の評価項目に注目
を移す
S33
NO
終り
YES
S34
次の関数ブロック図
に注目を移す
S35
YES
終り
NO
S36
計算結果の表示
S37
NO
保存する
YES
S38
結果保存
エンド

【図９】


600 メインダイアログボックス
602
601
603
608
関数読込
B
606
607
関数ファイル名
参照
自動組替
ON
OFF
609
610
計算実行
613
結果保存
611
612
結果ファイル名
参照
604
605
終了

【図１０】


スタート
S51
関数ブロック図、試行マス情報の入力
S52
試行マスに配置されている単位ブロック
と置換可能な単位ブロックの決定
S53
単位ブロックの置き換えによる
関数ブロック図の生成
S54
結果の出力
エンド

【図１１】

144 置換部品一覧

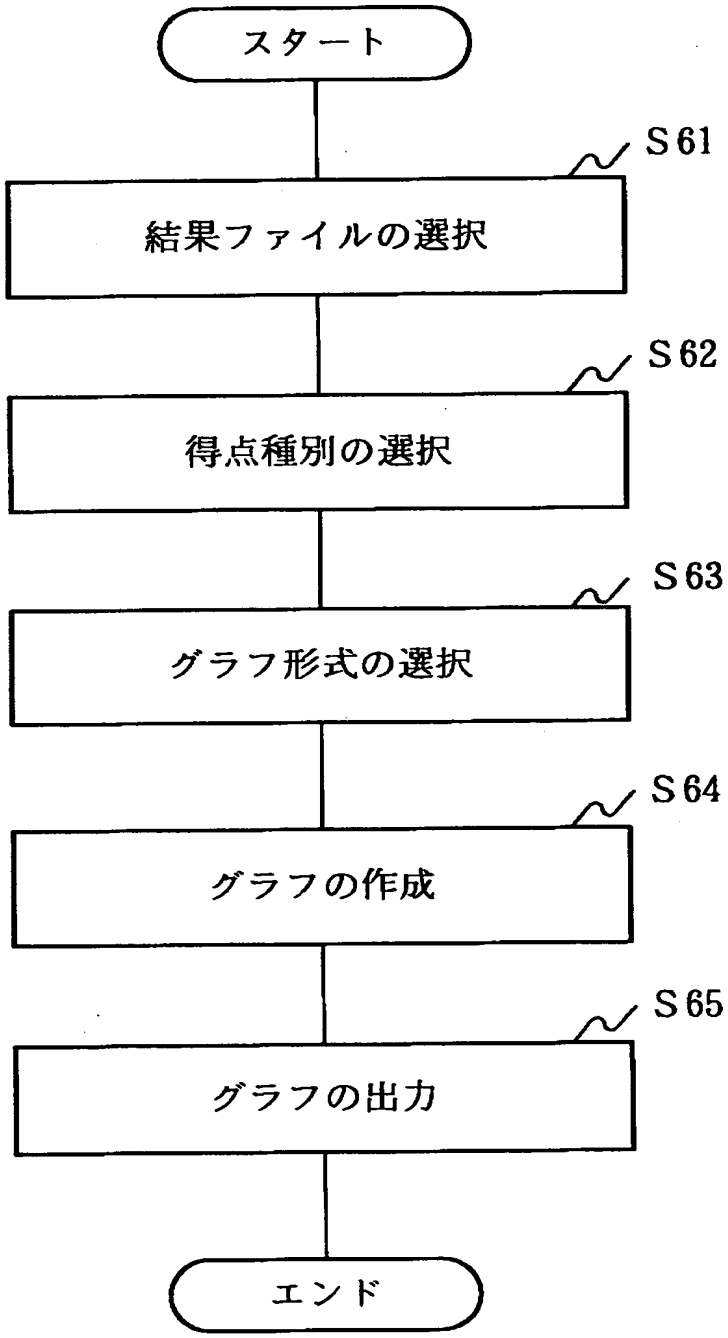
置き換え元	置き換え可能な基本ブロック
基本ブロック412	基本ブロック413、415、416、417
基本ブロック413	基本ブロック415、416、417、412
基本ブロック415	基本ブロック416、417、412、413
基本ブロック416	基本ブロック412、413、415、417
基本ブロック417	基本ブロック416、412、413、415
基本ブロック425	基本ブロック424
基本ブロック424	基本ブロック425
基本ブロック418	基本ブロック419
基本ブロック419	基本ブロック418
基本ブロック420	基本ブロック421
基本ブロック421	基本ブロック420

出証特２０００－３０８４３９９

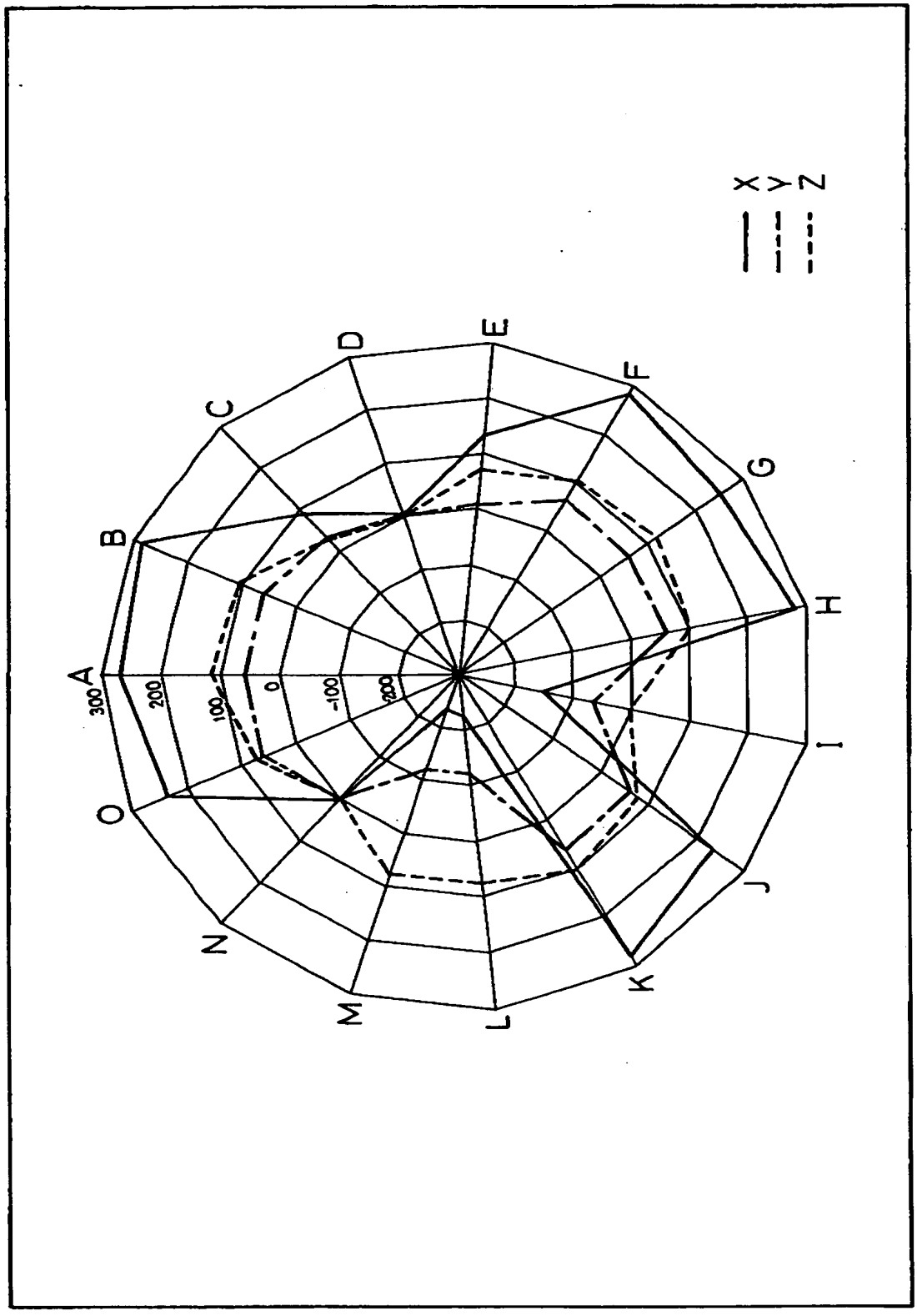
【図１２】

評価項目	基本ブロックの点数
A	
B	
・ ・ ・	
N	

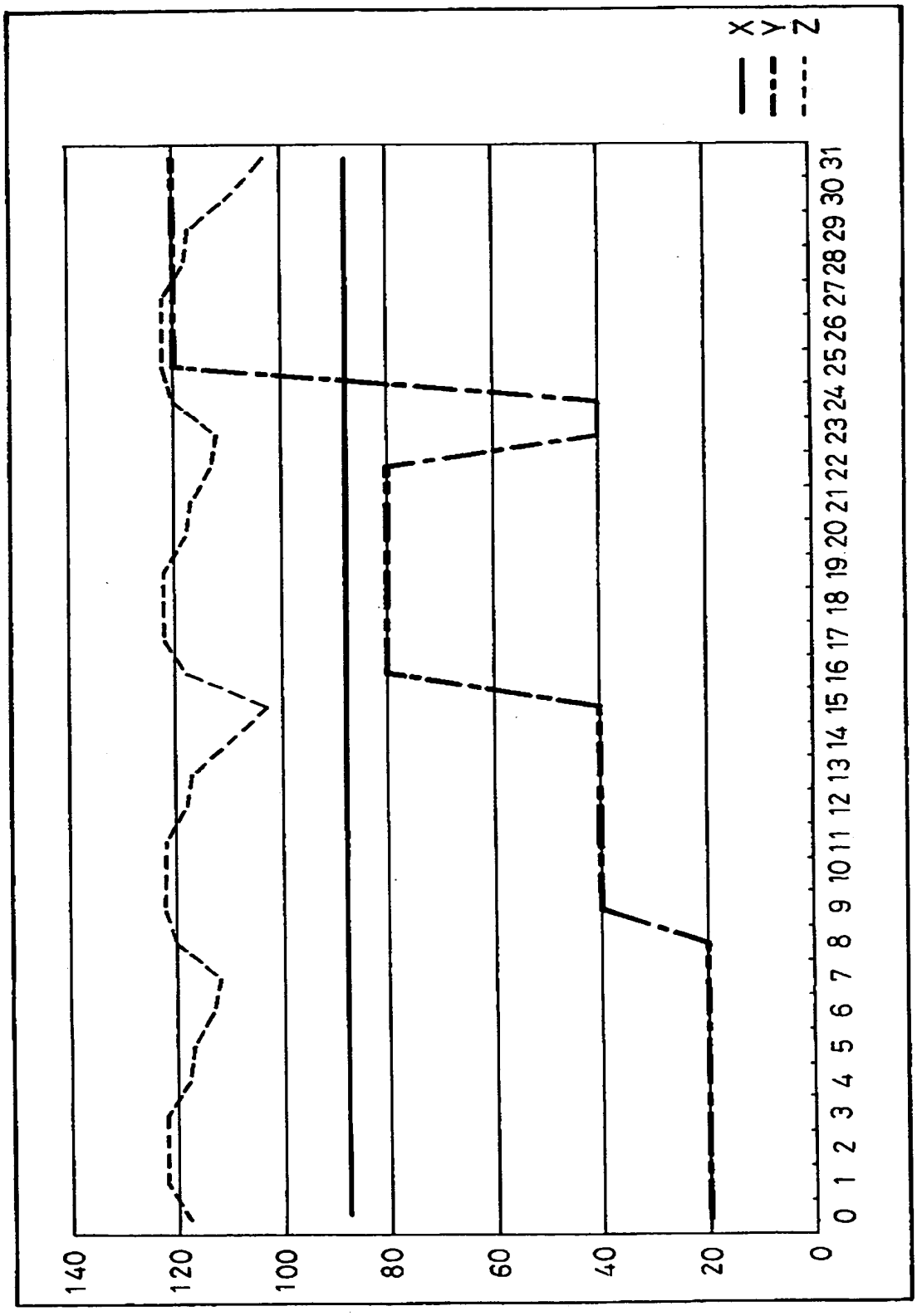
【図１３】


スタート
S61
結果ファイルの選択
S62
得点種別の選択
S63
グラフ形式の選択
S64
グラフの作成
S65
グラフの出力
エンド

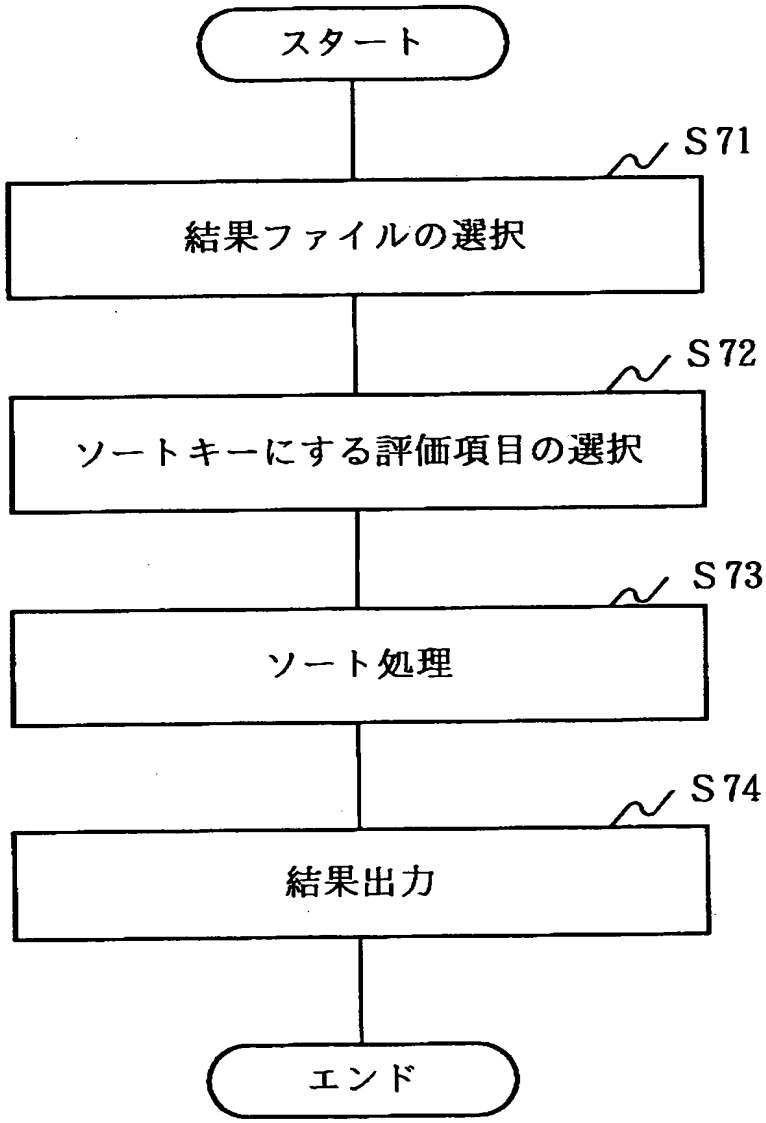
【図１４】



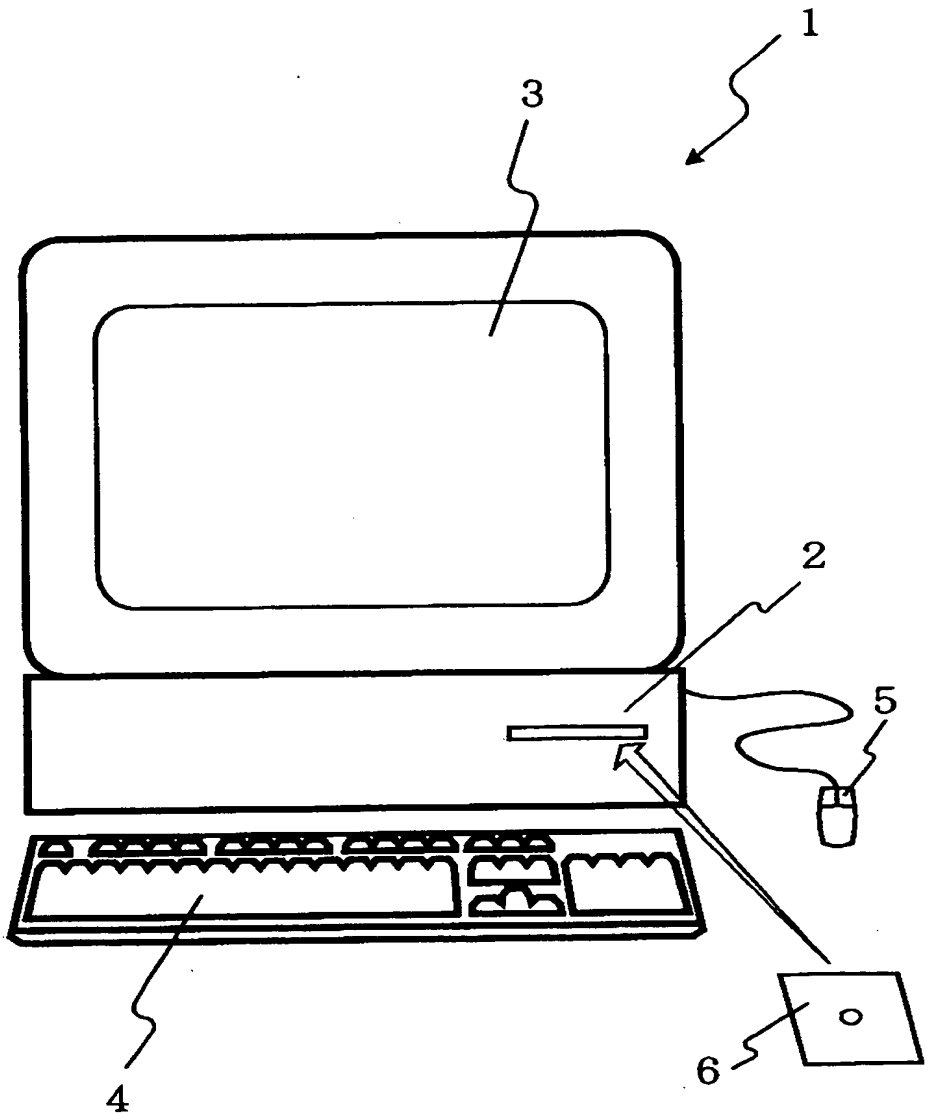
【図１５】


X
Y
Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
0
20
40
60
80
100
120
140

【図１６】


スタート
S71
結果ファイルの選択
S72
ソートキーにする評価項目の選択
S73
ソート処理
S74
結果出力
エンド

【図１７】



【書類名】　　要約書

【要約】

【課題】　暗号アルゴリズムの評価時間を大幅に短縮でき、かつ暗号設計の専門家でなくても強度評価などが行える暗号評価支援システムを提供する。

【解決手段】　点数記憶部142 には、予め定義した暗号アルゴリズム仕様記述法で使う単位図形の点数が暗号設計と評価の専門家の知識と経験をもとに事前に設定されている。評価対象記憶部141 には、前記暗号アルゴリズム仕様記述法で記述された暗号アルゴリズムの図形表現（関数ブロック図）が格納される。入力装置13からの利用者の指定に従い、評価実施手段112 は、評価対象記憶部141 から関数ブロック図を入力し、その中の単位図形に対して点数記憶部142 に記憶された点数を付与し、予め定められた計算ルールに従って関数ブロック図全体の得点を計算して表示装置12に出力する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社